UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/766,102	01/19/2001	Martin Thomas	10191/1663	8931

26646   7590   10/04/2005

KENYON & KENYON
ONE BROADWAY
NEW YORK, NY 10004

EXAMINER
BAUM, RONALD

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 10/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

<table>
<tr><td rowspan="2"></td><td colspan="2" align="center">Application No.</td><td colspan="2" align="center">Applicant(s)</td></tr>
<tr><td colspan="2">09/766,102</td><td colspan="2">THOMAS ET AL.</td></tr>
<tr><td rowspan="2">Office Action Summary</td><td colspan="2">Examiner</td><td colspan="2">Art Unit</td></tr>
<tr><td colspan="2">Ronald Baum</td><td>2136</td><td></td></tr>
</table>

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 July 2005*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

U.S. Patent and Trademark Office

PTOL-326 (Rev. 7-05)   Office Action Summary   Part of Paper No./Mail Date 09282005

DETAILED ACTION

1.   This action is in reply to applicant's correspondence of 15 July 2005.

2.   Claims 1-16 are pending for examination.

3.   Claims 1-16 remain rejected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed
> in the United States before the invention by the applicant for patent or (2) a patent granted on an application for
> patent by another filed in the United States before the invention by the applicant for patent, except that an
> international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this
> subsection of an application filed in the United States only if the international application designated the United
> States and was published under Article 21(2) of such treaty in the English language.

4.   Claims 1-16 are rejected under 35 U.S.C. 102(e) as being anticipated by Mirov et al, U.S.

Patent 6,138,236.

5.   As per claim 1; "A method for protecting a microcomputer system from manipulation of

data stored in a storage arrangement of the microcomputer system, the microcomputer system

including a microcomputer allocated to the storage arrangement, comprising the steps of:

    causing the microcomputer to

        access the storage arrangement for processing the data [Abstract, figure 1 and

    accompanying description, col. 1,lines 13-col. 2,line 4, col. 2,lines 7-63]; and

    before the storage arrangement is accessed, performing the steps of:

        assigning an individual identifier to one of

            the allocated microcomputer and

the storage arrangement,

generating a comparison code and

storing the comparison code in the storage arrangement as a function of the

individual identifier [Abstract, figure 1 and accompanying description, col. 1,lines 13-col.

2,line 4, col. 2,lines 7-63], and

at a time that is one of before and during an operation of the microcomputer system,

generating a security code as a function of the individual identifier and

comparing

the security code with

the comparison code [Abstract, figure 1-4 and accompanying descriptions,

col. 1,lines 13-col. 2,line 4, col. 2,lines 7-63],

wherein the microcomputer accesses the storage arrangement only if

the security code agrees with

the comparison code [Abstract, figure 1-4 and accompanying descriptions, col.

1,lines 13-col. 2,line 4, col. 2,lines 7-63, col. 4,lines 18-55, whereas the aspect of the

verification and data hashes generated and subsequently compared by the comparator

such that; a match occurring allows for the subsequent (permitted) booting/execution of

stored program data (and inherent access to said data) versus the not properly verified and

therefor not permitted to execute (and inherent restricted access to said data), clearly

encompasses the claimed limitations as broadly interpreted by the examiner.].";

Further, as per claim 10, this claim is the system claim for the method claim 1 above, and

is rejected for the same reasons provided for the claim 1 rejection, as such; "A storage

arrangement in which data are stored and to which is allocated at least one microcomputer that

accesses the storage arrangement for processing the data, comprising:

an arrangement for

storing a comparison code that is generated as a function of an individual

identifier assigned to one of

the at least one microcomputer and

the storage arrangement; and

an arrangement for,

at a time that is one of before and during an operation of the storage arrangement,

generating a security code as a function of the individual identifier and for

comparing

the security code with

the comparison code,

wherein the microcomputer accesses the storage arrangement only if

the security code agrees with

the comparison code.";

Further, as per claim 14, this claim is the system claim for the method claim 1 above, and

is rejected for the same reasons provided for the claim 1 rejection, as such; "A microcomputer

system, comprising:

a microcomputer: and

a storage arrangement assigned to the microcomputer, wherein:

data are stored in the storage arrangement,

the microcomputer accesses the storage arrangement in order to process

the data,

in the storage arrangement, a comparison code that is generated as a

function of an individual identifier assigned to one of

the microcomputer and to

the storage arrangement is stored, and

the microcomputer includes an arrangement for, at a time that is one of

before and during an operation of the microcomputer system,

for generating a security code as a function of the individual

identifier and to

compare

the security code with

the comparison code,

wherein the microcomputer accesses the storage arrangement only if

the security code agrees with

the comparison code.".

6.   Claim 2 *additionally recites* the limitation that; "The method according to claim 1,

wherein:

the data corresponds to a program.".

The teachings of Mirov et al suggest such limitations (Abstract, figure 1-4 and accompanying

descriptions, col. 1,lines 13-col. 2,line 4, col. 2,lines 7-63, whereas the "plurality of micro code"

is a stored program, and therefore clearly encompasses the claimed limitations as broadly

interpreted by the examiner.).

Further, as per claim 11, this claim is the system claim for the method claim 2 above, and

is rejected for the same reasons provided for the claim 2 rejection, as such; "The storage

arrangement according to claim 10, wherein:

the data correspond to a program.".

Further, as per claim 15, this claim is the system claim for the method claim 2 above, and

is rejected for the same reasons provided for the claim 2 rejection, as such; "The microcomputer

according to claim 14, wherein:

the data correspond to a program.".

7.   Claim 3 *additionally recites* the limitation that; "The method according to claim 1,

wherein:

a program stored in the storage arrangement is protected.".

The teachings of Mirov et al suggest such limitations (Abstract, figure 1-4 and accompanying

descriptions, col. 1,lines 13-col. 2,line 4, col. 2,lines 7-63, whereas the "security sensitive

environments require that the micro code be tamper proof..." constitutes a protected stored

program, and therefore clearly encompasses the claimed limitations as broadly interpreted by the

examiner.).

8.   Claim 4 *additionally recites* the limitation that; "The method according to claim 1,

wherein before the storage arrangement is accessed, the method further comprises the steps of:

        storing the individual identifier as

                the comparison code in the storage arrangement; and

        at the time that is one of before and during the operation of the microcomputer system,

performing a check as to whether

                the comparison code agrees with

                the individual identifier, used as the security code, of the allocated

        microcomputer.".

The teachings of Mirov et al suggest such limitations (Abstract, figure 1-4 and accompanying

descriptions, col. 1,lines 13-col. 2,line 4, col. 2,lines 7-63, col. 5,line 51-col. 8,line 26, whereas

the public key encryption oriented digital signature constitutes an individual identifier as the

comparison code, and therefore clearly encompasses the claimed limitations as broadly

interpreted by the examiner.).

9.   Claim 5 *additionally recites* the limitation that; "The method according to claim 1,

wherein:

        the storage arrangement normally cooperates with the allocated microcomputer only

when

the security code agrees with

the comparison code.".

The teachings of Mirov et al suggest such limitations (Abstract, figure 1-4 and accompanying

descriptions, col. 1,lines 13-col. 2,line 4, col. 2,lines 7-63, col. 5,line 51-col. 8,line 26, whereas

the public key encryption oriented digital signature comparison success allows for the boot-up

process to continue such that "...the trust level of the unsecured micro-code is raised to a level of

trusted, other boot data such as the boot blocks of the disk drive...", and thereby constitutes the

storage arrangement cooperating with the allocated microcomputer when the security code

agrees with the comparison code, and therefore clearly encompasses the claimed limitations as

broadly interpreted by the examiner.).

10.   Claim 6 *additionally recites* the limitation that; "The method according to claim 1,

wherein:

before an operation of the storage arrangement, after every start-up of the storage

arrangement,

the security code

is generated and

is compared with

the comparison code.".

The teachings of Mirov et al suggest such limitations (Abstract, figure 1-4 and accompanying

descriptions, col. 1,lines 13-col. 2,line 4, col. 2,lines 7-63, col. 5,line 51-col. 8,line 26, whereas

the public key encryption oriented digital signature comparison success allows for the boot-up

process to continue such that "...the trust level of the unsecured micro-code is raised to a level of

trusted, other boot data such as the boot blocks of the disk drive..." , and thereby constitutes the

storage arrangement cooperating with the allocated microcomputer when the security code

agrees with the comparison code, again, throughout the memory access functions during "start-

up of the storage arrangement", and therefore clearly encompasses the claimed limitations as

broadly interpreted by the examiner.).

11.   Claim 7 *additionally recites* the limitation that; "The method according to claim 6,

further comprising the step of:

    placing the storage arrangement in a mode in which,

        after every start-up, the storage arrangement is switched from

            an inactive state to

            an active state only when

                the security code agrees with

                the comparison code.".

The teachings of Mirov et al suggest such limitations (Abstract, figure 1-4 and accompanying

descriptions, col. 1,lines 13-col. 2,line 4, col. 2,lines 7-63, col. 5,line 51-col. 8,line 26, whereas

the public key encryption oriented digital signature comparison success allows for the boot-up

process to continue such that "...the trust level of the unsecured micro-code is raised to a level of

trusted, other boot data such as the boot blocks of the disk drive..." , and thereby constitutes the

storage arrangement cooperating with the allocated microcomputer when the security code

agrees with the comparison code, again, throughout the memory access functions during "start-

up of the storage arrangement", and therefore clearly encompasses the claimed limitations as

broadly interpreted by the examiner.).

Further, as per claim 12, this claim is the system claim for the method claim 7 above, and

is rejected for the same reasons provided for the claim 7 rejection, as such; "The storage

arrangement according to claim 10, wherein:

>the storage arrangement is capable of being, placed in a mode in which,

>>after every start-up, the storage arrangement is switched from

>>>an inactive state to

>>>an active state only when

>>>>the security code agrees with

>>>>the comparison code.".

Further, as per claim 16, this claim is the system claim for the method claim 7 above, and

is rejected for the same reasons provided for the claim 7 rejection, as such; "The microcomputer

according to claim 14, wherein:

>the microcomputer is capable of being placed in a mode in which,

>>after every start-up, the microcomputer is switched from

>>>an inactive state to

>>>an active state only when

>>>>the security code agrees with

>>>>the comparison code.".

12.   Claim 8 *additionally recites* the limitation that; "The method according to claim 6,

further comprising the step of:

  placing the allocated microcomputer in a mode in which,

    after every start-up, the allocated in microcomputer is switched from

      an inactive to

      an active state only when

        the security code agrees with

        the comparison code.".

The teachings of Mirov et al suggest such limitations (Abstract, figure 1-4 and accompanying

descriptions, col. 1,lines 13-col. 2,line 4, col. 2,lines 7-63, col. 5,line 51-col. 8,line 26, whereas

the public key encryption oriented digital signature comparison success allows for the boot-up

process to continue such that "…the trust level of the unsecured micro-code is raised to a level of

trusted, other boot data such as the boot blocks of the disk drive…", and thereby constitutes the

storage arrangement cooperating with the allocated microcomputer when the security code

agrees with the comparison code, again, throughout the memory access functions during "start-

up of the storage arrangement", and therefore clearly encompasses the claimed limitations as

broadly interpreted by the examiner.).

13.   Claim 9 *additionally recites* the limitation that; "The method according to claim 1,

further comprising the steps of:

  executing a validation program stored in

a read-only memory of the allocated microcomputer;

determining a code word in the validation program from

at least one part of a memory content of the storage arrangement in accordance

with a key; and

comparing

the code word with

a comparison code word stored in the storage arrangement.".

The teachings of Mirov et al suggest such limitations (Abstract, figure 1-4 and accompanying

descriptions, col. 1,lines 13-col. 2,line 4, col. 2,lines 7-63, col. 5,line 51-col. 8,line 26, whereas

the public key encryption oriented digital signature comparison success allows for the boot-up

process to continue such that "...the trust level of the unsecured micro-code is raised to a level of

trusted, other boot data such as the boot blocks of the disk drive...", and thereby constitutes the

storage arrangement cooperating with the allocated microcomputer when the security code

agrees with the comparison code, again, throughout the memory access functions during "start-

up of the storage arrangement", and therefore clearly encompasses the claimed limitations as

broadly interpreted by the examiner.).

14.   Claim 13 *additionally recites* the limitation that; "The storage arrangement according to

claim 10, wherein:

the storage arrangement corresponds to a flash memory.".

The teachings of Mirov et al suggest such limitations (Abstract, figure 1-4 and accompanying

descriptions, col. 1,lines 13-col. 2,line 4, col. 2,lines 7-63, whereas the "... flash PROM is

divided into two main sections..." is a storage arrangement corresponding to a flash memory, and therefore clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

Response to Amendment

15.   As per applicant's argument concerning the lack of teaching of security and comparison codes, both a function of the same individual identifier, the examiner has fully considered the arguments and finds them not to be persuasive. The firmware authentication prior to re-execution via a upgrade of same clearly encompasses the '... protecting a microcomputer system from manipulation of data stored in a storage arrangement of the microcomputer system...' [i.e., Abstract, col. 2,lines 7-33], as broadly interpreted by the examiner. Further, the predetermined digital signature clearly does corresponds to the applicant's use of the comparison code, as broadly interpreted by the examiner, in that the signature is pre-generated prior to access, and is clearly individualized relative to the memory signature (i.e., a unique checksum aspect of the memory arrangement would be inherent given a unique key and memory configuration per se.). The data and verification hash comparison clearly as part of the authentication process to run (any) software, let alone the upgraded software (i.e., the new firmware), again, clearly as broadly interpreted by the examiner, encompasses the teaching of the code comparison aspects of the claim limitation language. The claim language specifically dealing with the phrase 'individual identifier' is sufficiently broad such that checksums, memory individuality aspects of signature/hash considerations, would therefore be applicable in the rejection.

Conclusion

23.   Any inquiry concerning this communication or earlier communications from examiner

should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose

unofficial Fax number is (571) 273-3861. The examiner can normally be reached Monday

through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization

where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. For more information for

unpublished applications is available through Private PAIR only. For more information about the

PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

Primay Examiner

AU 2131

9/29/05